

Serial No.: 10/084,744
Docket No.: 40655.4100

Amendments To Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (currently amended) A PDA portal which facilitates securing ~~at least~~ a portion of content from a source to a PDA, wherein said PDA portal is configured to:

- receive a signal from said PDA indicating said portion of said content to be at least one of refreshed and downloaded;
- identify said PDA;
- interrogate said source containing said portion of said content to determine if when secure content is included in said portion of said content;
- connect to an encryption device, which is configured to ~~isolate imbedded links~~; establish a secure connection to said source using a negotiated encryption key, secure said portion of said content, receive encrypted content which is an encrypted portion of said content, decrypt said encrypted content, interrogate said content, isolate said imbedded links, re-encrypt said portion of said content and transmit said imbedded links and said encrypted content to said PDA portal;
- receive said imbedded links and said encrypted content from said encryption device; and,
- transmit said imbedded links and said encrypted content to said PDA for storage when said portion of said content has been collected from at least one of said source, wherein said encrypted content remains encrypted on said PDA.

Claims 2-3 (cancelled)

4. (currently amended) A PDA device which facilitates securing ~~at least~~ a portion of content from a source to said PDA, wherein said PDA is configured to:

- transmit a signal to a PDA portal, wherein said signal represents said portion of said content to be at least one of refreshed and downloaded to said PDA;
- provide identification signals to said PDA portal, wherein said PDA portal is configured to interrogate ~~sources~~ said source containing said portion of said content to determine if when secure content is included in said portion of said content;

Serial No.: 10/084,744

Docket No.: 40655.4100

connect to an encryption device, which is configured to ~~isolate imbedded links~~; establish a secure connection to said source using a negotiated encryption key, secure said portion of said content, receive encrypted content which is an encrypted portion of said content, decrypt said encrypted content, interrogate said content, isolate said imbedded links, re-encrypt said portion of said content and transmit said imbedded links and said encrypted content to said PDA portal;

receive said imbedded links and encrypted content from said hardware encryption device, and transmit said encrypted content to said PDA;

receive said imbedded links and said encrypted content from said PDA portal; and,

receive a pass-phrase from ~~said~~ a user to authenticate said user and decrypt said encrypted content.

5. (currently amended) The PDA device of claim 4, wherein said PDA device is configured to store said encrypted content ~~in an encrypted state~~ and receive a said pass-phrase from said user for each access to said encrypted content.

6. (currently amended) A method for securing ~~at least~~ a portion of content from a source to a PDA, said method comprising:

synchronizing said PDA to a PDA portal;

transmitting a signal to said PDA portal, wherein said signal represents said portion of said content to be at least one of refreshed and downloaded to said PDA;

providing identification signals from said PDA to said PDA portal, wherein said PDA portal is configured to interrogate ~~sources~~ said source containing said portion of said content to determine ~~if~~ when secure content is included in said portion of said content; ;

~~connect~~ connecting to an encryption device, which is configured to ~~isolate imbedded links~~; establish a secure connection to said source using a negotiated encryption key, secure said portion of said content, receive encrypted content which is an encrypted portion of said content, decrypt said encrypted content, interrogate said content, isolate said imbedded links, re-encrypt said portion of said content and transmit said imbedded links and said encrypted content to said PDA portal;

~~receive~~ receiving said imbedded links and encrypted content from said hardware encryption device; ~~and~~

~~transmit~~ transmitting said imbedded links and said encrypted content to said PDA;

receiving said imbedded links and encrypted content from said PDA portal;

Serial No.: 10/084,744
Docket No.: 40655.4100

storing said encrypted content ~~in encrypted form~~; and,
receiving a pass-phrase from said user to authenticate said user and decrypt said encrypted content stored in said PDA.

7. (currently amended) The method claim 6, wherein said step of receiving a said pass-phrase includes receiving a said pass-phrase from said user for each access to said encrypted content.

8. (currently amended) A method for facilitating secure collection of ~~at least~~ a portion of content from a source using a PDA portal, said method comprising:
receiving a signal indicating said portion of said content to be ~~at least~~ one of refreshed and downloaded;

interrogating said source containing said portion of said content to determine if when secure content is included in said portion of said content;

connecting to an encryption device, which is configured to ~~isolate imbedded links~~;
establish a secure connection to said source using a negotiated encryption key, secure said portion of said content, receive encrypted content which is an encrypted portion of said content, decrypt said encrypted content, interrogate said content, isolate said imbedded links, re-encrypt said portion of said content and transmit said imbedded links and said encrypted content to said PDA portal; and,

~~receive~~ receiving said imbedded links and said encrypted content from said encryption device; and,

transmitting said imbedded links and said encrypted content to said PDA for storage when said portion of said content has been collected from at least one of said source, wherein said encrypted content remains encrypted on said PDA.

Claim 9 (cancelled).

10. (currently amended) The method of claim 9 8, wherein said step of re-encrypting further comprises re-encrypting with ~~the~~ said encryption key of a PDA user.

11. (currently amended) A PDA portal which facilitates securing ~~at least~~ a portion of content from a source to a PDA, wherein said PDA portal is configured to:

receive a signal from the said PDA indicating said portion of said content to be at least one of refreshed and downloaded;

Serial No.: 10/084,744

Docket No.: 40655.4100

request secure content from a web site sites using a hardware encryption device, which is configured to: to receive the results of the requested content using a secure protocol; and
isolate imbedded links within the PDA Portal and identify the content to be secured;
establish a secure connection to said source using a negotiated encryption key, secure said
portion of said content, receive encrypted content which is an encrypted portion of said content,
decrypt said encrypted content, interrogate said content, isolate said imbedded links, re-encrypt
said portion of said content and transmit said imbedded links and said encrypted content to said
PDA portal; and,

transmit said imbedded links and the said encrypted content to the said PDA for storage
when said portion of said content has been collected from at least one of said source, wherein
said encrypted content remains encrypted on said PDA.

12. (currently amended) The PDA portal of claim 11, wherein said PDA portal is further configured to:

identify the said PDA;

interrogate the said source containing the said portion of the said content to determine if when said secure content is included in the said portion of the said content; and

encrypt the said content using the said hardware encryption device and a user pass-phrase.

13. (currently amended) A method for implementing a loyalty program using a PDA portal which facilitates securing at least a portion of content from a source to a PDA, the method comprising the steps of:

receiving and storing a manufacturer item identifier ~~identifiers~~;

receiving and processing a consumer ID;

receiving and processing purchase data, wherein said purchase data comprises at least a retailer item identifier;

associating said consumer ID, said purchase data, and a said manufacturer item identifier;

performing an analysis dependent upon the said step of associating said consumer ID, said purchase data, and said manufacturer item identifier;

synchronizing said PDA to a PDA portal;

Serial No.: 10/084,744
Docket No.: 40655.4100

transmitting a signal to said PDA portal, wherein said signal represents content to be at least one of refreshed and downloaded to said PDA and said signal includes at least one of said consumer ID, said purchase data, and said manufacturer item identifier;

providing identification signals from said PDA to said PDA portal, wherein said PDA portal is configured to interrogate said source sources containing said portion of said content to determine if when secure content is included in said portion of said content, connect to a hardware encryption device, which is configured to: isolate imbedded links by establishing a secure connection to said source using a negotiated encryption key, secure said portion of said content, receive encrypted content which is an encrypted portion of said content, decrypt said encrypted content, interrogate said content, isolate said imbedded links, re-encrypt said portion of said content and transmit said imbedded links and said encrypted content to said PDA portal; receive encrypted content from said hardware encryption device, and transmit said imbedded links and said encrypted content to said PDA;

receiving said encrypted content from said PDA portal;

storing said encrypted content in encrypted form when said portion of said content has been collected from at least one of said source, wherein said encrypted content remains encrypted on said PDA; and

receiving a pass-phrase from said a user to authenticate said user and decrypt said encrypted content.

14. (currently amended) A system for implementing a loyalty program on a network-wide level using a PDA portal which facilitates securing at least a portion of content from a source to a PDA, comprising:

~~means for associating~~ said PDA portal configured to associate a consumer ID, purchase data from multiple retailers, and a manufacturer item identifier,

wherein said purchase data comprises a retailer item identifier; and

wherein said PDA portal is configured to:

receive a signal from said PDA indicating content to be at least one of refreshed and downloaded and said signal includes at least one of said consumer ID, said purchase data, and said manufacturer item identifier;

identify said PDA;

Serial No.: 10/084,744
Docket No.: 40655.4100

interrogate said source containing said portion of said content to determine if when secure content is included in said portion of said content;

connect to an encryption device, which is configured to: isolate imbedded links by facilitating a secure connection to said source using a negotiated encryption key, securing said portion of said content, receiving encrypted content which is an encrypted portion of said content, decrypting said encrypted content, interrogating said content, isolating said imbedded links, re-encrypting said portion of said content and transmitting said imbedded links and said encrypted content to said PDA portal;

receive said encrypted content from said encryption device; and

transmit imbedded links and said encrypted content to said PDA for storage when said portion of said content has been collected from at least one of said source and a plurality of sources, wherein said encrypted content remains encrypted on said PDA; and,

~~means for performing~~ perform an analysis to calculate rewards points, said analysis being dependent upon an association of said consumer ID, said purchase data, and said manufacturer item identifier from said PDA.